

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X

In the Matter of an Application of the United
States of America for an Order Authorizing
the Use of Two Pen Register and Trap and
Trace Devices

MEMORANDUM & ORDER

Misc. 08-308

-----X
NICHOLAS G. GARAUFIS, United States District Judge.

This matter comes before the court as an appeal of Magistrate Judge James Orenstein's June 11, 2008 Amended Orders, in which Judge Orenstein authorized the issuance of two pen registers under the Pen Register and Trap and Trace Statute, 18 U.S.C. §§ 3121 et seq. ("Pen Register Statute"). In the Government's view, Judge Orenstein's denial of its request for post-cut-through dialed digits¹ along with other "significant caveats" in the Amended Orders effectively denied its application. (See Government's Appeal to the District Court, dated June 23, 2008 ("Gov. Br.") at 7, 9.)² In addition to its appeal of Judge Orenstein's decision, the Government has made a supplemental application directly to this court requesting prospective cell-site information which it did not request in its initial application before Judge Orenstein. (Government's Aug. 19, 2008 letter to the court, exhibit A.)

¹ As discussed below, post-cut-through dialed digits are digits that are dialed from a telephone after a call is connected or "cut through."

² The court is aware that all the Government's submissions have been filed ex parte and under seal in order to protect sensitive law enforcement information contained therein. It is necessary, however, for the court to set forth certain information stated therein. Thus, the court will refer to the Government's submissions throughout this opinion as necessary, but will not recount information from those submissions that might compromise the Government's investigatory techniques and procedures in general or divulge the details of the investigatory efforts in this case in particular.

As a result of several submissions made to this court by the Government, the legal issues presented by Judge Orenstein's "effective" denial of the Government's application are now moot. Therefore, the only significant legal issues presented here concern the Government's supplemental application for prospective cell-site information. Because of the complexity and significance of these legal issues, the court invited the Electronic Frontier Foundation ("EFF") to submit a memorandum of law as amicus curiae.

I. Judge Orenstein's Amended Orders

On June 11, 2008, the Government applied to Judge Orenstein for authorization to install and use a pen register and trap and trace device on two wireless telephones (the "SUBJECT WIRELESS TELEPHONES"). (Gov. Br. at 5.) The Government requested, *inter alia*, an Order authorizing the recording of post-cut-through dialed digits ("PCTDD") via pen register. PCTDD are digits dialed from a telephone after a call is connected or "cut through." In the Matter of Applications, 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007) ("Azrack Opinion"). Because PCTDD sometimes transmit information such as bank account numbers and Social Security numbers which constitutes "contents of communications," and because the Pen Register Statute defines a pen register as "a device or process which *records or decodes* dialing . . . or signaling information . . . provided, however, that *such information shall not include the contents of any communication*," 18 U.S.C. § 3127(3) (emphasis added), Judge Orenstein denied the Government's request for authorization to record PCTDD. The Government subsequently appealed Judge Orenstein's denial of its request to this court, asking this court to authorize it to record PCTDD.

On September 23, 2008, in response to the court's request for clarification of the specifics of its request for pen register data, the Government informed the court that the law enforcement

agency involved in the investigation of the SUBJECT WIRELESS TELEPHONES will configure its computers so as to immediately delete all PCTDD received from the provider. (Government's September 23, 2008 letter to the court.) Therefore, as the pen registers sought by the Government in this application will not "record" or "decode" content within the meaning of the Pen Register Statute, the legal question presented by the Government in its appeal is moot.³ As the Government is entitled to the information it now seeks, the court directs the Magistrate Judge to issue, if still necessary, an order authorizing the installation of the pen registers on the SUBJECT WIRELESS TELEPHONES that is consistent with the representations in the Government's letter of September 23, 2008.

II. The Government's Request for Prospective Cell-Site Information

On August 19, 2008, after it appealed Judge Orenstein's Amended Orders, the Government made a supplemental application to this court for prospective cell-site information.⁴ (Government's August 19, 2008 letter to the court, ex. A.) In its application, the Government seeks prospective cell-site information pursuant to the so-called "hybrid theory," under which the Government argues that it is authorized to receive cell-site information pursuant to the combined

³ It is irrelevant that the provider will forward PCTDD to the Government and that the Government will therefore be able, if it violates the court order, to record and decode it. The court trusts that the Government does not violate court orders. In any case, Congress, in Title III, has clearly expressed its belief that the Government can without supervision limit its investigatory activities so as to protect the constitutional rights of suspects. See 18 U.S.C. § 2518(5) (every order "shall contain a provision that the authorization to intercept shall be . . . conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter.")

⁴ As discussed below, cell-site information is information that discloses which antenna towers are receiving signals from a particular cellular telephone at any point in time when the cellphone is powered on. If received on a prospective basis, this information can be used to track the location of the cellphone and its user in the future. Historical cell-site information, on the other hand, can be used to track the previous movements of a cellphone and its user. Judge Orenstein granted the Government's request for historical cell-site information in his June 11, 2008 Amended Orders. (See Sealed Order of Authorization (Gov. Br., ex. D) at 2-3, 5.)

authority of the Pen Register Statute and the Stored Communications Act (“SCA”), 18 U.S.C. § 2701 et seq. Many district and magistrate judges around the country have considered this theory. Courts are divided, with a majority denying the Government’s requests. See In the matter of the Application, 534 F. Supp. 2d 585, 599-600 (W.D. Pa. 2008) (“Lenihan Opinion”) (collecting cases), aff’d, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008). This court joins the minority of courts in concluding that the Government may obtain, without a showing of probable cause, the cell-site information it requests pursuant to the combined authority of the Pen Register Statute and the SCA.

A. The Hybrid Theory

When a cellular telephone is on, regardless of whether it is making or receiving a voice or data call, it “periodically transmits a unique identification number to register its presence and location in the network.” In re Application, 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006) (“Kaplan Opinion”). This signal, as well as the signals associated with calls made by that phone, is received by every antenna tower within range of the phone. Id. The general location of the phone can then be determined based upon the location of the antenna tower receiving these signals, sometimes “with a fair degree of precision” if they are received by two or more antenna towers simultaneously. Id. at 451.⁵ Cellular telephone service providers record the identity and location of the antenna towers receiving signals from each phone, regardless of whether those phones are making voice or data calls, in order to determine whether roaming charges apply and in order to track call volume by location. Id. For obvious reasons, such information, known as cell-site information, is also useful to the Government as an investigatory tool. Id. at 451-52.

⁵ Current technology allows tracking of a cellphone’s location using cell-site information to within fifty feet. Lenihan Opinion, 534 F. Supp. 2d at 602.

Under the hybrid theory, the Government contends that the Pen Register Statute, which provides it with the authority to install and use a pen register, defined as “a device or process which records or decodes . . . signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,” see 18 U.S.C. 3127(3), also allows it to receive cell-site information. See In re Application, 405 F. Supp. 2d 435, 438-39 (S.D.N.Y. 2005) (“Gorenstein Opinion”). The Government concedes, however, that it may not obtain cell-site information under the authority of the Pen Register Statute alone because of an exception contained in the Communication Assistance for Law Enforcement Act (“CALEA”) of 1994, which requires telecommunications carriers to ensure that their equipment is capable of providing law enforcement agencies with information to which they may be entitled under statutes relating to electronic surveillance. Id. at 440. In relevant part,

a telecommunications carrier shall ensure that its equipment, facilities, or services . . . are capable of expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier . . . *except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).*

47 U.S.C. § 1002(a)(2) (emphasis added).⁶

As the argument goes, Congress’s use of the word “solely” in this exception means that, while the Government may not obtain cell-site information under the authority of the Pen

⁶ As Magistrate Judge Gorenstein has pointed out, this exception clause reflects the underlying assumption that “physical location data *would* have been obtainable under the Pen Register Statute in the absence of the exception clause. Otherwise, it would have been unnecessary to add the exception clause at all.” Gorenstein Opinion, 405 F. Supp. 2d at 440 (emphasis in original). Judge Gorenstein has also noted that, notwithstanding the fact that the operative definition of a pen register at the time CALEA was enacted did not seem to include cell-site information, the legislative history of Section 1002 suggests that Congress thought such information was available under the Pen Register Statute at the time it enacted the exception clause. Id. at 441 & n.4.

Register Statute alone, it may obtain cell-site information pursuant to the Pen Register Statute and some other, albeit unnamed, statute. See Gorenstein Opinion, 405 F. Supp. 2d at 440-42. More specifically, some courts have suggested that Section 1002's use of "solely" was predicated on a desire not to preclude the Government from seeking cell-site information, but rather on a desire to impose "an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices." See, e.g. id. at 443 (quoting United States Telecom Ass'n v. F.C.C., 227 F.3d 450, 463 (D. C. Cir. 2000) (approving the FCC's interpretation of the statutory language in this manner). The Government argues that Section 2703 of the SCA is an appropriate mechanism to "combine" with the Pen Register Statute to allow the Government to obtain cell-site information.

Sections 2703(c)(1) and 2703(d) of the SCA provide that a "governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)," provided the governmental entity "offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought are relevant and material to an ongoing criminal investigation."⁷ An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). The phrase "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. §

⁷ The SCA's requirement of specific and articulable facts showing reasonable grounds is higher than the Pen Register Statute's requirement that an attorney for the Government certify that the information "likely to be obtained is relevant to an ongoing criminal investigation being conducted." 18 U.S.C. § 3122(b)(2).

2510(12). However, “electronic communication . . . does not include . . . any communication from a tracking device,” 18 U.S.C. § 2510(12)(C), which is defined in Section 3117(b) of Title 18 as any “electronic or mechanical device which permits the tracking of the movement of a person or object.”

As noted above, many cases have considered the exact issue before this court. Having reviewed the statutory framework, the decisions granting and denying such requests, and the legislative history of the statutes, I find persuasive the detailed analysis contained in Magistrate Judge Gorenstein’s and Judge Kaplan’s opinions from the Southern District of New York. I am particularly persuaded that the use of the term “solely” in Section 1002 of CALEA is intended to guard against obtaining cell-site information under the Pen Register Statute’s minimal “relevant to an ongoing criminal investigation” standard, rather than to prohibit obtaining cell-site information completely. The SCA provides such a standard by requiring the Government to present “specific and articulable facts” in support of applications requesting cell-site information.

In addition, I am persuaded that the definition of the phrase “electronic communication” in the SCA, which excludes information from a tracking device, is immaterial to the question of whether the Government may obtain “a record or other information pertaining to a subscriber or customer of” such an electronic communication service under Section 2703 of the SCA. I agree with Judges Kaplan and Gorenstein that “record or other information” are the relevant terms in Section 2703, that cell-site information clearly qualifies as “information,”⁸ and that the term

⁸ EFF argues in its amicus brief that prospective cell-site information is not a “record or other information” within the meaning of Section 2703(c), because those terms refer to already-existing “historical” data. (EFF Brief at 25-28.) The prospective cell-site information sought by the Government, however, becomes a “historical record” as soon as it is recorded by the provider. Because the SCA in no way limits the ongoing disclosure of records to the Government as soon as they are created, the cell-site information the Government seeks is subject to disclosure to the Government pursuant to Section 2703(c).

“electronic communication service” has a meaning independent of the meaning of “electronic communication.” See Kaplan Opinion, 460 F. Supp. 2d at 460 & n.55. This is in contrast to those courts that agree with the Kaplan/Gorenstein analysis to this point, but then conclude that, because the definition of “electronic communication” excludes information from a tracking device, cell-site information cannot be the kind of “record or other information” accessible under Section 2703. See, e.g., In the Matter of the Application, 497 F. Supp. 2d 301, 311 (D.P.R. 2007) (rejecting Judge Kaplan’s approach and concluding that “the court would have to judicially amend the statute to remove the definition of ‘electronic communication’ found at Section 2510(12) for the tracking device exception *not* to apply . . . I cannot prune the definition of ‘electronic communication’ from ‘electronic communication service.’”)

Judge Kaplan opines that incorporating the definition of “electronic communication” into the term “electronic communications service” would have unintended consequences because the term “electronic communication” excludes “*any* communication from a tracking device, not just those communications that permit tracking.” Kaplan Opinion, 460 F. Supp. 2d at 460 & n.55. Applying this definition, any information a cellphone provides to a telecommunications carrier would not qualify as “electronic communication,” rendering such carriers not an “electronic communication service.” Id. The result of a telecommunications carrier not qualifying as an “electronic communication service,” Judge Kaplan concludes, is that the carrier “would have no obligation to disclose *any* information to the government under Section 2703(c). Accordingly, this reading virtually eviscerates Section 2703(c).” Id. This unintended consequence lends substantial support to the conclusion that the definition of “electronic communication” does not apply to Section 2703.

An argument made by EFF that has not been considered in the previous decisions adopting the Government's hybrid theory is that the doctrine of constitutional avoidance compels its rejection. Under this doctrine, a court "should construe an ambiguous statute to avoid constitutional problems if a viable alternative interpretation exists." United States v. Awadallah, 349 F.3d 42, 55 (2d Cir. 2003).

[I]t is a cardinal principle of statutory interpretation . . . that when an Act of Congress raises a serious doubt as to its constitutionality, [courts should] first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.

Zadvydas v. Davis, 533 U.S. 678, 689 (2001) (internal citations omitted).

It is clear that the hybrid theory is not the only way that the Pen Register Statute and the SCA may be construed. See In the Matter of the Application, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) (the hybrid theory "simply is not found in the plain language of any of the three statutes upon which the government relies"). Moreover, Congress has not provided the kind of guidance as to the correct manner of combining the Pen Register Statute with the SCA that might be expected if Congress intended such a combination. See Gorenstein Opinion, 405 F. Supp. 2d at 443 ("The idea of combining some mechanism with as yet undetermined features of the Pen Register Statute is certainly an unattractive choice. After all, no guidance is provided as to how this 'combination' is to be achieved."); Kaplan Opinion, 460 F. Supp. 2d at 461 (noting that the statutes' lack of any direct authorization for the combination of authority the Government proposed, while not fatal to the Government's application, was "somewhat troubling"). Therefore, if the court had serious doubts as to the constitutionality of the SCA and the Pen Register Statute, as construed using the hybrid theory, the court would be compelled by the doctrine of constitutional avoidance to reject the hybrid theory.

The interesting aspect of EFF's argument is that the "serious doubts" EFF is concerned about arise not in the present case, but in a hypothetical future case in which the Government might, pursuant to the hybrid theory, request far more detailed tracking information that would allow precise tracking of a target inside his or her home. According to EFF, the hybrid theory, so applied, would be unconstitutional because it would contravene the holding of the Supreme Court in United States v. Karo, 468 U.S. 705, 714-18 (1984), prohibiting warrantless location tracking of a person inside the person's home. (EFF Br. at 35.) The specter of such precise location tracking does not loom over this case, because the Government is seeking only information identifying the one antenna tower (and portion of such tower) receiving transmissions from the SUBJECT WIRELESS TELEPHONES at the beginning and end of calls made from those phones. (Government's Aug. 19, 2008 letter to the court, exhibit A.) Such information, unlike the information revealed by triangulation or by more advanced communications devices like the iPhone, which contain Global Positioning System devices, is not precise enough to enable tracking of a telephone's movements within a home. EFF argues, however, that this court should take into account in this case the possibility that in future cases the hybrid theory could be used to justify the disclosure of more precise tracking information.

In Clark v. Martinez, 543 U.S. 371, 380-81 (2005), the Supreme Court held that the serious constitutional doubts triggering application of the doctrine of constitutional avoidance need not arise in the controversy before the court:

It is not at all unusual to give a statute's ambiguous language a limiting construction called for by one of the statute's applications, even though other of the statute's applications, standing alone, would not support the same limitation. The lowest common denominator, as it were, must govern . . . In other words, when deciding which of two plausible statutory constructions to adopt, a court must consider the necessary consequences of its choice. If one of them would raise a multitude of constitutional problems, the other should prevail – whether or

not those constitutional problems pertain to the particular litigant before the Court.

(internal citations omitted).

In Clark, the Supreme Court considered a statute, Section 1231(a)(6) of Title 8, which allows for the continued detention of an inadmissible alien subject to a removal order after a 90-day period in which the Secretary of Homeland Security is supposed to remove the alien from the United States has elapsed. In Zadvydas, an earlier case, the Supreme Court, considering aliens who had been admitted to the United States before later being ruled inadmissible, construed the statute so as to allow such continued detention only while removal was still reasonably foreseeable. 533 U.S. at 689-90. This construction, the Supreme Court held, was required by the doctrine of constitutional avoidance. Id. In Clark, the Supreme Court considered the application of the same statute to aliens who had never been admitted to the United States. 543 U.S. at 378. Even though such an application arguably did not give rise to serious constitutional doubts, the Court held that the same statute could only have one construction, and therefore that a court applying the doctrine of constitutional avoidance had to consider the universe of possible applications of the statute in question, not only the application of the statute in the present cause. Id.

The court finds, for several reasons, that Clark v. Martinez is inapposite here. First, the hypothetical situation creating constitutional problems is far more hypothetical in the present case than in Clark. Whereas the statute considered in Clark and Zadvydas by its terms explicitly applied both to aliens previously found admissible and aliens who had never been found inadmissible, and it was clear that the statute would routinely be applied to both groups of aliens, here there is no assurance that a court will ever be confronted with an application that would present serious constitutional problems. It is entirely in the Government's discretion to

determine the scope of the disclosure of information it seeks, and the Government may very well restrict itself to single-tower location information, like that sought in the present case, which would never allow tracking precise enough to lead to constitutional problems.

Second, applications under the Pen Register Statute and the SCA, which directly implicate Fourth Amendment concerns, are uniquely suited to case-by-case decision. Whereas an alien can be detained under Section 1231(a)(6) upon an exercise of discretion of the Secretary of Homeland Security, each application for disclosure under the hybrid theory must be approved by a federal judge – an official uniquely suited to consider constitutional problems and to limit possible future unconstitutional investigatory intrusions by the Government. See 18 U.S.C. § 2703(d) (requirements for court order under SCA); 18 U.S.C. § 3122 (application for a judicial order authorizing the installation and use of a pen register). In Sibron v. United States, the Court has noted that “[t]he constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case.” 392 U.S. 40, 60 (1968).⁹ Given this background principle of Fourth Amendment jurisprudence, the court declines to rule preemptively that a whole class of warrantless searches is constitutionally invalid.

Third, in a field like search and seizure law, where lawmakers are continually struggling to update legislation to cope with changing technology, the presumption, inherent in the doctrine

⁹ The court in Sibron expressly distinguished “the question of the adequacy of the procedural safeguards written into a statute which purports to authorize the issuance of search warrants in certain circumstances,” which it suggested, citing Berger v. New York, 388 U.S. 41 (1967), was a proper focus of a facial attack. As Congress has not here demonstrated its intention to promulgate a general statute purporting to authorize, without regard to constitutionality, all types of location tracking, the court does not believe that it is proper to consider the constitutionality of the hybrid theory “on its face.” Such consideration is more properly undertaken incrementally, as judges exercise their authority to determine the constitutionality of discreet applications made by the Government pursuant to the hybrid theory.

of constitutional avoidance, that Congress did not intend to promulgate legislation which “raises serious constitutional doubts,” see Clark, 543 U.S. at 381, has little applicability. At the time that Congress promulgated the Pen Register Statute and the SCA, it could only speculate as to the changing technology which might increase the universe of information available to the Government under those acts. Congress therefore wisely made disclosure under both of those acts subject to the interposition of a judicial official, who could make sure that the Government’s requests complied both with constitutional and statutory prerequisites.

Although I understand the hesitance of some judges to grant the Government’s requests because of the lack of any express indication that the Pen Register Statute should be combined with the SCA, I am satisfied that CALEA clearly contemplates some combination of the Pen Register Statute and an additional statute to allow the Government to access and retrieve the cell-site information requested in this application. This conclusion is buttressed by Congress’s most recent indication of its intent with respect to cell-site information, namely that its inclusion of “signaling information” in the Pen Register Statute’s 2001 revision of the definition of a pen register contemplates giving the Government access to cell-site information. See Gorenstein Opinion, 405 F. Supp. 2d at 438-49; see also United States Telecom Ass’n, 227 F.3d at 463-64 (holding that cell-site information constitutes “signaling information”); Kaplan Opinion, 460 F. Supp. 2d at 456 (presuming that Congress knew when it added the term “signaling information” to the definitions of pen registers and trap and trace devices in 2001 that the D.C. Circuit had interpreted that term to include cell-site information a year earlier). Congress’s lack of clarity as to the appropriate mechanism and standard the Government must meet in order to obtain cell-site information is less troubling inasmuch as it has made clear that the Government should be able to obtain cell-site information by some mechanism. Furthermore, as Judge Kaplan points out, the

Pen Register Statute and the SCA have “interconnected histories” — Congress enacted both in 1986 as part of the Electronic Communications Privacy Act and amended both with CALEA in 1994 — which suggests that it is not unreasonable to use them in conjunction even in the absence of a specific directive from Congress to do so. See Kaplan Opinion, 460 F. Supp. 2d at 461.

Having reached this conclusion, I join in Judges Gorenstein’s and Kaplan’s concern, not to mention the concern of those judges denying the Government’s requests, over Congress’s lack of clear guidance on this issue. See Gorenstein Opinion, 405 F. Supp. 2d at 443 (“The idea of combining some mechanism with as yet undetermined features of the Pen Register Statute is certainly an unattractive choice. After all, no guidance is provided as to how this ‘combination’ is to be achieved.”); Kaplan Opinion, 460 F. Supp. 2d at 461 (noting that the statutes’ lack of any direct authorization for the combination of authority the Government proposed, while not fatal to the Government’s application, was “somewhat troubling”). I also join in suggesting that Congress “may wish to consider whether this result is consistent with its intention.” Kaplan Opinion, 460 F. Supp. 2d at 450. District courts across the country are divided on an issue that requires balancing the Government’s investigatory needs with citizens’ right to privacy. Absent clarity from Congress, this division and inconsistency in outcomes will continue because the issue is one about which reasonable judges can, and obviously do, disagree.

Based upon the foregoing conclusions, I grant the Government’s application for cell-site information. It has presented, under seal, specific and articulable facts showing reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation. See 18 U.S.C. 2703(d). This Order authorizes telephone service providers to provide the Government with information which identifies the antenna tower receiving

transmissions from the SUBJECT WIRELESS TELEPHONES at the beginning and end of a particular call made or received by the SUBJECT WIRELESS TELEPHONES' users, including information on what portion of that tower is receiving a transmission at the beginning and end of a particular call. This Order does not permit the Government to receive triangulation information or location information other than that transmitted at the beginning and end of particular calls. Additionally, for the reasons stated in Part I of this Memorandum and Order, the court directs the Magistrate Judge to issue, if still necessary, an Order authorizing the installation of the pen registers on the SUBJECT WIRELESS TELEPHONES that is consistent with the representations in the Government's letter of September 23, 2008.

SO ORDERED.

Dated: Brooklyn, New York
November 22, 2008

s/Nicholas G. Garaufis

NICHOLAS G. GARAUFIS
United States District Judge